Claims

What is claimed is:

1. A multiplier, comprising:

a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form; and

a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a two's complement form, wherein

the Wallace tree block comprises:

a sum calculation block adding the partial products, and

a carry calculation block adding carries generated by the sum calculation block.

2. The multiplier according to claim 1, wherein a result of the calculation of the sum calculation block is outputted as a result of the multiplication over an extension field of two.

3. The multiplier according to claim 1, wherein the carry propagation adder adds a result of the calculation of the sum calculation block and a result of the calculation of the carry calculation block and outputs a result of the addition as a result of the multiplication for integers.

4. The multiplier according to claim 1, wherein the sum calculation block performs multiply and add operations by adding another value for each corresponding digit to the partial products.

5. A multiplier multiplying two input values as objects of multiplication by calculating partial products for the two input values and adding the partial products using half adders and full adders, the multiplier comprising:

multiplication means for calculating a sum of the partial products and outputting the sum as a result of the multiplication in the case that the input values are elements in an extension field of two;

carry addition means for adding carries generated in the calculation of the multiplication means; and

addition means for adding a result of the calculation of the multiplication means and a result of the calculation of the carry addition means and outputting a result of the addition as the result of the multiplication in the case where the input values are integers.

6. The multiplier according to claim 5, wherein the multiplication means collects and outputs only addition terms by an exclusive OR operation, addition terms being outputted from the half adders and the full adders.

7. The multiplier according to claim 6, wherein the carry adder means collects terms other than the addition terms added by the multiplication means and performs addition including the carry terms and the addition terms by the half adders and the full adders.

8. The multiplier according to claim 6, wherein a multiply and add operation is performed by adding the addition terms of the partial products in the multiplication means to other addition terms.

9. A cipher circuit, comprising:

arithmetic means for performing arithmetic for encryption or decryption of data; and

control means for controlling the arithmetic by the arithmetic means;

wherein the arithmetic means comprise a multiplier using half adders and full adders and comprises:

a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form; and

a carry propagation adder converting a redundant binary number outputted from the Wallace tree block to a two's complement form; and

wherein the Wallace tree block comprises:

a sum calculation block adding the partial products, and

a carry calculation block adding carries generated by the sum calculation block.

10. The cipher circuit according to claim 9, wherein the arithmetic means outputs a result of the calculation of the sum calculation block in the case of arithmetic over a finite field $GF(2^n)$ and outputs a result of the calculation of the carry calculation block in the case of arithmetic over a finite field GF(p).

11. The cipher circuit according to claim 9, wherein the sum calculation block collects and outputs only addition terms by an exclusive OR operation outside of the arithmetic means, the addition terms being outputted from the half adders and the full adders.

12. The cipher circuit according to claim 9, wherein the carry calculation block collects terms other than addition terms added by the multiplication means and performs addition including the carry terms and the addition terms by the half adders and the full adders.

13. A cipher circuit, comprising:

arithmetic means for performing arithmetic for encryption or decryption of data; and

control means for controlling the arithmetic by the arithmetic means;

wherein the arithmetic means comprises a multiplier which multiplies two input values as objects of multiplication by calculating partial products for the input values and adding the partial products using half adders and full adders and the arithmetic means comprises:

multiplication means for calculating a sum of the partial products for each digit and outputting the sum as a result of the multiplication in the case that the input values are elements of a finite field $GF(2^n)$; and

carry addition means for adding carries generated in the calculation of the multiplication means; and

addition means for adding a result of the calculation of the multiplication means and a result of the calculation of the carry addition means and outputting a result of the addition as a result of the multiplication in the case where the input values are integers.